FORM PTO-1390
(REV. 9-2001)

U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER
PAGA06US

U S APPLICATION NO (If known, see 37 CFR 1 5)
10/018943

INTERNATIONAL APPLICATION NO. PCT/BY99/00005	INTERNATIONAL FILING DATE 27 APRIL 1999	PRIORITY DATE CLAIMED 27 APRIL 1999

TITLE OF INVENTION
METHOD FOR ENCRYPTING INFORMATION AND DEVICE FOR REALIZATION OF THE METHOD

APPLICANT(S) FOR DO/EO/US MISCHENKO, VALENTIN A.; ZAKHARAU, ULADZIMIR U.; VILANSKI, YURI V.; and VERZHBALOVICH, DZMITRY

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Aplication under PCT Article 19 (35 U S.C. 371(c)(3))
   a ☐ are attached hereto (required only if not communicated by the International Bureau)
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☐ Other items or information:

U.S. APPLICATION NO (if known, see 37 CFR 1.5) 10/018943	INTERNATIONAL APPLICATION NO PCT/BY99/00005	ATTORNEY'S DOCKET NUMBER PAGA06US

21. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1040.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$890.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$740.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$710.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 1040	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 ☒ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ 130	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	18 -20 =	0	x **$18.00**	$ 0	
Independent claims	4 -3 =	1	x **$84.00**	$ 84	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$280.00**	$ 280	

TOTAL OF ABOVE CALCULATIONS =	$ 1534	
☒ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +	$	
SUBTOTAL =	$	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).	$	
TOTAL NATIONAL FEE =	$ 767	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$	
TOTAL FEES ENCLOSED =	$ 767	
	Amount to be refunded:	$
	charged:	$

a. □ A check in the amount of $ ______________ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 14-0783 in the amount of $ 767 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 14-0783 A duplicate copy of this sheet is enclosed.

d. □ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO.

DAVID NEWMAN CHARTERED
P.O. BOX 2728
LA PLATA, MD 20646

TE: 301 934-6100

David B Newman Jr
SIGNATURE

DAVID B NEWMAN JR
NAME

30,966
REGISTRATION NUMBER

Attorney Docket: PAGA06US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of)
)
MISCHENKO et al)
)
Intern'l App. No. PCT/BY99/00005) Group Art Unit:
)
I.A. Filed: 27 APR. 1999) Examiner:
)
For: METHOD FOR ENCRYPTING)
INFORMATION AND DEVICE FOR)
REALIZATION OF THE METHOD)
)

Box PCT
Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

PRELIMINARY AMENDMENT A

Prior to calculating the application fee, amend the application as follows:

IN THE CLAIMS:

Amend the claims as follows:

5. The method according to claims 1, 2, or 3, [or 4], characterized [characterised] in that the certain part of the accessory data for the [said] cycle (F_i) is added to the transformed in the [said] cycle data (C_i) in each or some transformation cycles.

Add the following claim:

--12. The method according to claim 4, characterized in that the certain part of the accessory data for the cycle (F_i) is added to the transformed in the cycle data (C_i) in each or some transformation cycles.--

REMARKS

By this Amendment, applicants amend claim 5, and add claim 12. Claims 1-12 are pending in the application.

Replacement copies of claims 5, and new claim 12 are attached herewith. Kindly enter this amendment prior to calculating the filing fee.

Respectfully submitted,

DAVID NEWMAN CHARTERED

By: David B Newman
David B. Newman, Jr.
Registration No. 30,966

Date: October 26, 2001

T:\PAG-BY\PAGA06US_AM1.wpd

LAW OFFICES
DAVID NEWMAN
CHARTERED
CENTENNIAL SQUARE
P.O. BOX 2728
LA PLATA, MD 20646
(301) 934-6100

5. The method according to claims 1, 2, or 3, characterized in that the certain part of the accessory data for the cycle (F_1) is added to the transformed in the cycle data (C_1) in each or some transformation cycles.

12. The method according to claim 4, characterized in that the certain part of the accessory data for the cycle (F_1) is added to the transformed in the cycle data (C_i) in each or some transformation cycles.

METHOD FOR ENCRYPTING INFORMATION AND DEVICE FOR REALIZATION OF THE METHOD

The invention relates to means for protecting information from an unauthorized access, and may be used in crypto-systems for encoding, transferring and decoding communications, and in other systems for protection of information.

The prior art discloses engineering solutions providing protection of transmitted information by means of a special equipment or encoding software, for example by using scrambler for protection of telephone conversations [1] pp. 35-37, Fig. 22. The scrambler operates on the principle on inversion of an audio signal. As a result of an inversion a usual speech turns to a senseless gang of sounds, but the initial signal is accepted by the user without any distortion. The telephone set is equipped with the block for voice modification controlled by the encoder. The encoder stores 13122 user's codes providing 52488 digital combinations. The read-only memory of the set stores the resident software, which codes and decodes the transmitted information in several variants and controls the work of the whole set.

However this prior art solution has problems in providing a fair degree of secrecy, since for disclosing the confidential codes it is enough to execute a limited number of mathematical operations that are fast and effectively executed by the modern high-speed electronic engineering.

The main characteristic of a crypto-system is the degree of secrecy. The task of a cryptographer is to provide the utmost secrecy and authenticity of the transferred information. Alternatively, a crypto-analyst "forces open", or "breaks", the crypto-system designed by a cryptographer. The crypto-analyst tries to decipher the set of encoded symbols and to deliver the encrypted communication as the plaintext.

Prior art discloses technical solutions for protecting the transferred information by using a specific device and/or encoding software. Known codes are based on two simple methods: substitution and interchange. Interchange uses simple mixing of plain-text symbols, the key of an interchange encryptor defines the specific type of mixing. The frequency distribution of individual symbols in the encoded text is identical to that of the plaintext. For substitution, each symbol of the plaintext is replaced by another symbol of the same alphabet, and the specific type of substitution is determined by the secret key.

For example, the algorithm in the Data Encryption Standard (DES) [2], p. 33-34 uses the both methods. The algorithm comprises plaintext, unencrypted text and the key as binary sequences having the length 64, 64 and 56 bits, respectively. When DES is used in an electronic book or table mode, the 64-bit blocks of the plaintext are encoded independently by using one key. The algorithm of DES includes 16 rounds or cycles, each of which has simple interchanges combined with substitution in four-bit groups. In each pass, 48 key bits are selected in a pseudo-random manner from the full 56-bit key.

The problem of DES is that this prior art solution does not provide a fair degree of secrecy, since for disclosure of such secret codes with possible number of 2^{64} keys combinations, substituting of all keys during a brute-force attack using modern computer techniques is performed in an acceptable time. Also, using the same plaintext and not varying the keys, produces the same encoded text. Analysis reveals the statistical regularity of the correlation between the plaintext and the encoded text, and may allow decoding the encoded text without using direct substitution of all the keys.

A crypto-system using public keys RSA is described in [2] p. 37-39. This system uses a one-way function - discrete logarithms raising to a power.

GOST P. 34.11 - 94 [3], p. 3-8 discloses hatching consisting in comparing an optional set of data as a sequence of binary symbols, with a short, fixed length image thereof. In this system 64-bit subwords are encoded using keys of 256 bit length.

The drawbacks of these systems are small the key length, which may permit decoding during acceptable time, and a slow decoding speed. These systems are practically stable systems.

Theoretically stable systems have perfect secrecy. According to Shannon [4] p. 333-402, that means that the plaintext, and the encoded text or cryptogram, are statistically independent for all plaintext and cryptograms.

A prior art Vernam crypto-system is a theoretically stable crypto-system. Theoretically stable systems make certain demands on a key. For a system with closed keys the indeterminacy of the key should not be less than the indeterminacy of the plaintext. In theoretically stable systems the length of a key should be not less than the length of the plaintext. In the Vernan system the key length is equal to the length of the plaintext. This system was used in a code-notebook [5] for transfer of one encoded text. This is the main drawback of a codebook because the key should be changed and delivered with every transfer.

There are known crypto-systems using the so-called randomisers [2] p. 26 - 27. A randomiser is a software or a hardware device that encodes some symbols of plaintext with some random plurality of codes.

Typically, this is done for providing equal frequency of the plaintext alphabet. Symbol frequency equalisation is required so that a crypto-analyst cannot organise decoding of a plaintext based on analysis of frequency characteristics of a cryptogram. For a random plaintext and a random selection of a code, a derandomiser should correctly determine the initial symbol without transfer of information from the randomiser location. In classical systems with a small randomising field, this task is solved by substituting codes belonging to the randomised symbol. Randomisers, however, do not play a substantial role in crypto-protectability of an encoding system, as secret keys are the main means of protection.

Under the combination of the essential features the most close prior art object to the claimed method and device is the disclosed in [6] the device and method of encoding that use a pnnciple of full randomizing symbols of the initial alphabet on a plurality of codes with potencies of large dimensionality, The said prior art invention was selected by the inventors for the prototype of the claimed invention.

In respect of a method the selected for the prototype object is a method of encoding and transferring information, wherein the addressee is beforehand provided for a key to the received communications with information on regularities corresponding to the values of the communication transmitted to him, with specific values of the initial information for the whole set of symbols of the said kind of an information, processing an information using the said regularities and transferring to the addressee the communication containing data, obtained during processings information, the values of transmitted data, which depend on random generated numbers being calculated during processing information, characterized in that the addressee is beforehand provided with a set of functions $Y_1...Y_n = Y_i(X)$, where X is a variable, and each Yi corresponds to a specific symbol of information, and also with the support function U = U (Z), where Z is a variable, and with the key function W = W (Y, U), where Y and U are variables accepting values of any of the values from the values of the said functions Yi and U, in the course of processing of a transmitted information for each symbol there are generated two random numbers X and Z, the respective value of Y is calculated on basis of the respective function Yi (X) for a specific symbol, the value of U is further calculated on basis of the support function U (Z), the value of W for this symbol is calculated on basis of the key function W (Y, U) and obtained for the symbol value of Y and the value of U from the support function, and the addressee is transmitted the communication containing data on the thus obtained values of W, X and Z for each symbol of the initial information.

In respect of a device, the object selected for the prototype is a device for realizing a method of encoding and transferring information, which comprises a unit for information input, a set of symbols, a data base on regularities connecting the specific symbols with the communication, which data base is supplied with a calculator connected to the generator of random numbers, the device further comprising the encoder and the unit for recording and transmitting communications, and the encoder being connected to the set of symbols and calculator output, the device further comprising a unit for calculating the values of the support function and a unit for calculating the values of the key function, the generator of random numbers is supplied with two outputs joint with the encoder, the first output of the generator of random numbers is connected also to the input of the unit for calculating values of the support function, and second – to the input of the calculator of the data base on regularities, the output of this calculator is connected to the encoder through the unit for calculating values of the key function, and the second input of the latter is connected to the output of the unit for calculating values of the support function.

However the problem of object selected for the prototype is that in the course of the encryption the length of the encrypted communication exceeds the length of the initial communication by several times.

The aim of the claimed invention is providing an improved method of encrypting by means of obtaining several communications from one initial, at least one of the obtained communications may be compressed up to preset sizes so that any connection between the initial text and the cryptogram is completely is lost for a cryptoanalyst.

As a result of the solution of the problem there is achieved a new technical effect consisting in creating a new system of encrypting that ensures a high crypto-stability of a system without any increase of the length of the communication.

The said technical effect is achieved as follows.

1. The method of encrypting of an information comprises the following steps:

- Preliminary generation of information on regularities connecting the values of symbols of the initial communication with the specific values of the encrypted communication for the total set of values of the said kind of communications;
- determination the number (n) of transformation cycles of the initial communication;
- realization of the transformation cycle comprising:
- generation of the feature (Ri), defining regularity used for transformation of the communication in the current transformation cycle;
- transformation of the communication with use of the selected regularity;
- repetition of transformation cycles the certain number of times;
- transformation of the communication in each cycle being realized in a way resulting in forming a communication (Ci), transformed in the said cycle and the accessory information for the said cycle (Fi);
- the number (n) of transformation cycles of the initial communication is selected from the preset criterion,
- forming the encrypted communication consisting of two parts, one of which contains the finally transformed communication (Cn), and second one contains a set of the accessory information (F = {F1, F2, ..., Fn}).

2. The further improvement of the method is characterized by that:

- transformation of the communication in each cycle is realized in a way resulting in forming a communication (Ci) transformed in the said cycle, being of the shorter or equal length with the initial communication, and resulting in forming an accessory information for the said cycle (Fi);
- the number (n) of transformation cycles of the initial communication is selected from the preset criterion (for example, the size of the finally transformed communication),
- forming the encrypted communication consisting of two parts, one of which contains the finally transformed communication (Cn) being of the shorter length

with the initial communication, and second one contains a set of the accessory information (F = {F1, F2, ..., Fn}).

3. Still further improvement of the method is characterized by that:

- transformation of the communication in each cycle realizes in a way resulting in forming a communication (Ci) transformed in the said cycle, being of the shorter, equal or longer length with the initial communication, and resulting in forming an accessory information for the said cycle (Fi);
- the number (n) of transformation cycles of the initial communication is selected from the preset criterion (for example, the size of the finally transformed communication),
- forming the encrypted communication consisting of two parts, one of which contains the finally transformed communication (Cn) being of the shorter, equal or longer length with the initial communication, and second one contains a set of the accessory information (F

4. The further improvement of a method is characterized by that in each or some cycles the communication (Ci) transformed in the said cycle and (or) an accessory information for the said cycle (Fi) are intermixed.

5. The following improvement of the method is characterized by that in each or some cycles of transformation the certain part of an accessory information for the said cycle (Fi) is added into the transformed in the said cycle communication (Ci).

The structural interpretation of stated ideas could be considered on an example of the claimed device.

The device for a realizing the method of encrypting information comprises:

- an input unit,
- an output unit, the first input of which is connected to the second output of the commutator, and the second — to the output of the accessory information storage ;
- data base on the regularities connecting the initial information with the encoded information, the first input of the said data base being connected to the first output of the input unit and the second input – to the output of the random numbers generator;
- a random number generator, the input of which is connected to the first output of the making decision unit;

- the transformation unit, the first input of which is connected to the second output of the output unit, the second input – to the output of the data base, and the third input –to the first output of the commutator;
- the storage for the transformed information, the input of which is connected to the first output of the transformation unit;
- a storage for the accessory information, the first input of which is connected to the second output of the transformation unit, and the second input – to the second output of the making decision unit;
- the making decision unit, the first input of which is connected to the third output of the input unit, the second input – to the first output of the storage for the transformed communication;
- the commutator, the first input of which is connected to the second output of the storage for the transformed communication, and the second input – to the second output of the making decision unit.

1. The method of decoding encrypted information comprises the following steps:

- preliminary generating data on regularities connecting values of all encoded symbols that may be used in the said kind of information with initial symbols, which are identical to the regularities used at encoding;
- extracting, from the encoded communication, of the data (R_i), defining the regularity which is used in the current transformation cycles and connects the values of the encoded communications with the concrete symbols of the transformed information of the current transformation cycle;
- selecting the regularity connecting the values of the encoded communications with the concrete symbols of the transformed information of the current transformation cycle;
- extracting from the accessory information (F) the accessory information for the said transformation cycle (F_i);
- transforming the transformed information (C_i) using the selected regularity and the accessory information for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;
- the accessory information for the said transformation cycle (F_i); being isolated from the array of the accessory information (F);

- recovering the information (C_i), which is transformed in the respective cycle, by using the selected regularity and the accessory information for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;
- using additionally in each transformation cycle a respective part of the accessory information, as a result of transforming with the use of the selected regularity there is formed the information recovered in the respective cycle.

2. The further improvement of a method is characterized by that:

- in each transformation cycle there is additionally used a respective part of the accessory information and as a result of the transformation with use of the selected regularity there is formed a recovered in the corresponding cycle communication, the length of which is larger or equal to the length of the communication, resulting from transforming in the previous cycle.

3. The following improvement of a method is characterized by in each transformation cycle there is additionally used a respective part of the accessory information, and as a result of transformation with use of the selected regularity there is formed a recovered in the respective cycle communication, the length of which is larger, equal or smaller than the length of the communication, resulting from transforming in the previous cycle.

4. One more improvement o the method is characterized by that the transformed in the respective cycle information (C_i) and/or the accessory information for the respective cycle (F_i) is preliminary unmixed in each cycle or in some cycles;

The device for realizing the method of decoding of the communication, comprises:

- an input unit,
- an output unit,
- data base on the regularities connecting the encoded information with the initial information,
- a transformation unit;
- a storage of the recovered communication;
- a storage of the accessory information;
- a making decision unit;
- a commutator,

the first input of the accessory information storage being connected with first output of the input unit and the second input of the accessory information storage being connected with first output a making decision unit; the first input of data base is connected to the second output of the of the input unit, and the second input – to the first output of the storage for accessory information; the first input of the storage of the recovered information is connected to the third output of the input unit, the second – to the output of the transformation unit, and the third – to the first output of the making decision unit, the first input of the transformation unit is connected to the second output of the storage of accessory information, and the second – to the output of database, the third to the first output of the storage of recovered information; the second - to the fourth output of the input unit, the first input of the commutator is connected to the second output of the making decision unit, and the second – to the second output of the making decision unit, the output unit is connected to the second commutator output .

With the first output (exit) of the switchboard; the first input (entrance) of the block of a decision making is connected to the first output (exit) of an accumulator of the restored communication, and second — With the fourth output (exit) of the block of input; the first input (entrance) of the switchboard is connected to the second output (exit) of the block of a decision making, and second — With the second output (exit) of an accumulator of the restored communication; the block of a conclusion is connected to the second output(exit) of the switchboard.

The distinctive feature of the new method can be illustrated by the following example. Symbols of the initial alphabet A {a1, a2, ..., an} being such, that the binary representation of each symbol has the identical length for the whole alphabet A, are substituted with symbols of the alphabet Bi {b1i, b2i, ..., bni} being such, that the binary representation of each symbol may have a various length, the process of such replacement is iterative, i. e. at each i-step for the initial communication there is used a result of the substitution obtained at the i-1step, at each i-step there is used its own substitution alphabet Bi, produced with the help of the function Yi, selected by a casual mode from a plurality of functions transferred to the addressee beforehand, and at each i-step there is produced the accessory information Fi used for restoring the initial communication is produced. As an additional measure of protecting from cryptanalysis, on each step or on some steps there may be performed intermixing of the communication resulting from the transformation. In an outcome of such transformation there is produced a transformed text (Cn), length of which may be not than the less length of one symbol of the alphabet Bn, used at the last step of transformation.

Such systems have uncommon properties:

- as a result of transformation of the initial communication there are produced at least two output communications (the transformed communication (Cn) and the accessory information (F), each of which separately has not any sense from the point of view of restoring the initial communication and may be transmitted through a separate data link;
- generally, the length of the transformed communication may have the length of one symbol of the substitution alphabet, for example if the initial communication has the byte representation, the transformed communication may have the one byte length, regardless of the length and kind of the initial communication;
- at multiple encoding one and the same initial communication the transformed communication will be various, eliminating thereby a problem of the closed channel for the key information transfer;
- The modification of ay symbol in the transformed communication or accessory information brings about the impossibility of restoring the initial communication.

The transformation functions (Yi) may be preset in the form of a table. For example, in case of representing the initial communication as N-bit binary sequences and transformation of compression of the function Yi, can be preset as a set of 2^N triples — {(ak, bik, fik)}, where ak is an N-bit initial code, bik is a transformed bit code of a variable length not greater N, and only two values of {bik} have the length of N bit, fik is the information on the length of the respective bik in bits. At such representation there exist such submission exist $(2^N)!(2^N-1)(2^N-2)$ of various possible functions of transformation such, that $\sum_{i=1}^{2^N} L_{ik} = \min L_{ik}$, where - L_{ik} - is length of bik in bits. At N = 8 there is present ≈256! *254*255 10^{511} of various transformation functions (Yi). In this case two values of bik have the one bit length, four values of bik have the two bit length, eight values of bik have the three bit length, sixteen values of bik have the four bit length, a thirty two values of bik have the five bit length, sixty four values of bik have the six bit length, one hundred twenty eight values of bik have the seven bit length and two values of bik have the eight bit length.

Then for an arbitrary function Yi the average length of the transformed communication X will be equal:

$$L(C_i(X,Y_i)) = L(X)\frac{2N + \sum_{n=1}^{N-1} n2^n}{N2^N}$$

and the average length of an accessory information:

$$L(F_i(X,Y_i)) = L(X)\frac{2N + \sum_{n=1}^{N-1} n2^{N-n}}{N2^N}$$

thus the average compression ratio at one step of transformation will have the values:

$$K_{core} = \frac{L(C_i(X,Y_i))}{L(X)} = \frac{2N + \sum_{n=1}^{N-1} n2^n}{N2^N}$$, for the transformed communication

$$K_{flags} = \frac{L(F_i(X,Y_i))}{L(X)} = \frac{2N + \sum_{n=1}^{N-1} n2^{N-n}}{N2^N}$$, for the accessory information.

In particular, for N = 8 we have: $K_{core} = 777/1024\ 0.758$ $K_{flags} = 255/1024$

At performing transformation M cycles the anticipated average length of the transformed communication will be:

$L(C(X)) = K_{core}^{M} L(X)$,

and of the accessory information -

$$L(F(X)) = L(X)K_{flags}\sum_{m=0}^{M-1} K_{core}^{m} = K_{flags}L(X)\frac{K_{core}^{M} - 1}{K_{core} - 1}$$.

Accordingly at performing 10 transformation cycles the average length of the transformed communication at of N = 8 will make approximately 0,067 of the length of the initial communication, and length of the accessory information — 0.97 of the length of the initial communication. The general length will make approximately 1.037 of the initial length, and for 100 transformation cycles — 10^{-12} and 1.04 accordingly.

If at each transformation cycle a S byte of the accessory information is added to the transformed communication, then average length of the transformed communication will be:

$$L(C(X)) = K_{core}^{M} L(X) + S\sum_{m=0}^{M} K_{core}^{m} = K_{core}^{M} L(X) + S\frac{K_{core}^{M+1}-1}{K_{core}-1},$$

And length of an accessory information will make:

$$L(F(X)) = \sum_{m=1}^{M} K_{flags}\left(K_{core}^{m} L(F) + S\frac{K_{core}^{m+1}-1}{K_{core}-1}\right) = \frac{K_{flags}}{1-K_{core}}\left(L(X)(1-K_{core}^{M}) + S\left(M-\frac{K_{core}^{M+2}-1}{K_{core}-1}\right)\right)$$

The construction of the claimed device may be realized in various variants realizing the claimed method of encoding information by using the known hardware. All these variants expand technological possibilities of using of the invention.

The main problem of the prototype method is eliminated thereby, i.e. essential increase of the sizes of the encrypted communication in a comparison with the initial one. The disclosed distinctive features of the claimed invention, in a comparison with known engineering solutions allow designing a device of encoding information providing statistical independence of the encrypted text and the open text, i.e. having properties of the theoretically stable of proof system of cryptography, and not by recurrence of the encrypted communication at repeated encoding of one and the same communication at constant keys.

Fig.1 shows a diagram of the device illustrating realization of a claimed method of encoding information is represented. Through the input unit the data base enters the pre- generated information on regularities connecting values of symbols of the initial communication with specific symbols of the encrypted communication for the whole set of symbols of the said kind of the communications. In the course of processing the encrypted information the input of the making decision unit (3) enters the information on the number (n) of transformation cycles of the initial communication. Before the beginning of the current transformation cycle, the making decision unit (3) transmits a control signal to the generator of random numbers (5), which generates a random number (Ri), transmits it to the data base (2) and through the latter- to the transformation unit. In accordance with the value of Ri from the database (2) there is selected the transformation function of YRi which enters the transformation unit (4). The transformation unit (4) calculates s the values of (Ci, Fi) = YRi (Xi, Ri). The value of Ci enters the input of the storage of the transformed communication (6) from outputs of the transformation unit (4) and the value of Fi enters the input of the storage of the accessory information (7). The storage of the transformed communication (6) transmits a signal on termination of the current cycle of transformation to the making decision unit (3). The making decision unit (3) makes a decision on fulfillment of the next transformation cycle or on terminating the process of transformation. In case of decisionmaking on the terminating the process of transformation the transformed information (Cn) through the switchboard (8) and the accessory information F = {F1, F2, ..., Fn} from the storage of an accessory information (7) enters the output unit (9). Otherwise the transformed communication (Ci) through the switchboard (8) enters in the transformation unit (4) for fulfillment the next cycle of transformation.

Fig. 2 shows the diagram of the device illustrating realization of the claimed method of decoding information. Through the input unit (10) into the data base (2) come the previously generated information on regularities connecting values of symbols of the initial communication with special symbols of the encrypted communication for the whole set of symbols of the said kind of the communications, which are identical to the regularities used at encoding. In the course of restoring the transformed communication through the input unit (10) enter the following data: at the input of the decision making unit (11) - information on the number (n) of transformation cycles of the deencrypted communication; at the storage of the accessory information (14) – the accessory information; at the storage of the restored communication (13) – the transformed communication. Before the beginning of the current cycle of restoring at the signal of the decision making unit (11) the storage of the accessory information (14) yields the accessory information (Fi) into the transformation unit (12) and the value of Ri – into the data base (2), in accordance with which is selected the function of transformation of Yri that arrives at the transformation unit (12), and the storage of the restored communication (13) yields through the switchboard (8) the transformed communication (Ci) into the transformation unit (12). The transformation unit (12) calculates the values of (Xi)) YRi (Ci, Fi). From the output of the transformation unit (12) the restored communication (Xi)) arrives into the storage of the restored communication (13). At completion of accumulation of the restored communication (Xi)) the storage of the restored communication (13) sends a signal on termination of the current cycle of restoring into the decision making unit (11). In case of decision-making on the termination of process of transformation the restored communication (Xi)) through the switchboard (8) arrives to the output unit (15). Otherwise from the output of the decision-making unit (11) at the input of the storage of the accessory information (14) arrives the signal on yielding of the next portion of the accessory information (Fi, Ri) and the restored communication arrives through the switchboard (8) at the transformation unit (12) for fulfillment of the next cycle of restoring.

Bibliographic data of sources of information

1. Victor Gavrish "Practical Guide on Protecting Commercial Secrets". Simferopol, TAVRIDA, 1994, p.35-37.
2. . Schmidt M. E., Bransted D.K. "Standard of Data Encoding: Past and Future" Journal of Works of Electronic and Radio Engineers (TIIER), 1988, v.76, no. 5., p. 33-34.
3. GOST 34.11-94 Information Technology, Crypto Graphical Protection of Information, Cash function. M.: Gosstandart of Russia, 1994, 34.11 - 94, p. 3-8.
4. Shannon C. E.. "Communication Theory in Secret Systems". Shannon C. E. "Works on Information and Cybernetics Theory". M.: IL, 1963, p. 333-402, “Theoretically Stable system,”, as cited in “An Introduction to Contemporary Cryptology”, Proceedings of the IEEE, v. 76. No. 5, May 1998.
5. Vernan. Copher printing telegraph systems for secret wire and radio telegraphic communications. // J Amer. Inst. Elec. Eng., vol. 55, pp. 109-115, 1926.
6. Mischenko V.A, Zakharov V.V. A method of encoding and transfer information and the device for a realization the method // Official Gazette of the Belarusian Patent Office. No.4, part I, 1997
7. Golubev V.V. Computer crimes and protection of information in computing systems // News in life, science and engineering. Part. Computer engineering and use thereof. Protection of information.- M.: Znanie, 1990.

Claims

1. A method for encoding information comprising the steps of:

- preliminary generating data on regularities connecting values of all initial symbols that may be used in the said kind of information with encoded symbols;
- determining the number (n) of cycles of transforming specific initial information;
- realising the cycle of transforming which comprises:
- generating the feature (R_i) that determines the regularity used for transforming the information in the current transformation cycle;
- transforming the information using the selected regularity;
- repeating transformation cycles a certain number of times;

- *characterised in that,*
- transforming of the information in each cycle is performed in such a way that results in forming a transformed in the said cycle information (C_i) and the accessory information for the said cycle (F_i);
- the number (n) of cycles of the transformation of the initial information is selected from the preassigned criterion,
- forming an encoded message consisting of two parts, one of the said parts comprises the finally transformed information (C_n), and the second one comprises the accessory information array ($F = \{F_1, F_2, \ldots, F_n\}$).

2. The process for encoding information according to claim 1, *characterised in that*

- transforming the information in each cycle is performed in such a way that results in forming a transformed in the said cycle information (C_i), that is shorter or equal to the length of the initial information, and the accessory information for the said cycle (F_i);
- the number (n) of cycles of the transformation of the initial information is selected from the preassigned criterion determining the size of the finally transformed information,
- forming an encoded message consisting of two parts, one of the said parts comprises the finally transformed information (C_n) that is shorter than the length of the initial communication, and the second one comprises the accessory information array ($F = \{F_1, F_2, \ldots, F_n\}$).

3. The process for encoding information according to claim 1, *characterised in that*

- transforming the information in each cycle is performed in such a way that results in forming a transformed in the said cycle information (C_i) that is shorter, equal or longer than the length of the initial information and the accessory information for the said cycle (F_i);
- the number (n) of cycles of the transformation of the initial information is selected from the preassigned criterion, determining the size of the finally transformed information and/or the degree of protectability of information,
- forming an encoded information consisting of two parts, one of the said parts comprises the finally transformed information (C_n) that is shorter, equal or longer than the length of the initial communication, and the second one comprises the accessory information array ($F = \{F_1, F_2, \ldots, F_n\}$).

4. The method according to claims 1, 2 or 3, *characterised in that* the transformed in the said cycle information (C_i) and/or the accessory information for the said cycle (F_i) are mixed in each cycle or in some cycles.
5. The method according to claims 1, 2, or 3, or 4, *characterised in that* the certain part of the accessory information for the said cycle (F_i) is added to the transformed in the said cycle information (C_i) in each or some transformation cycles.
6. The device for realising the process for encoding of information, comprises:

- an input unit,
- an output unit, the first input of which is connected with the second output of the commutator, and the second — with the output of the accessory information storage ;
- data base on the regularities connecting the initial information with the encoded information, the first input of the said data base being connected with the first output of the input unit and the second input – with the output of the random numbers generator;
- *characterised in that*, the device further comprises
- a random number generator, the input of which is connected with the first output of the making decision unit;
- the transformation unit, the first input of which is connected with the second output of the output unit, the second input –with the output of the data base, and the third input –with the first output of the commutator;
- the storage for the transformed information, the input of which is connected with the first output of the transformation unit;

- a storage for the accessory information, the first input of which is connected with the second output of the transformation unit, and the second input – with the second output of the making decision unit;
- the making decision unit, the first input of which is connected with the third output of the input unit, the second input – with the first output of the storage for the transformed communication;
- the commutator, the first input of which is connected with the second output of the storage for the transformed communication, and the second input – with the second output of the making decision unit.

7. The process for decoding of the encoded information comprising the steps of:

- preliminary generating data on regularities connecting values of all encoded symbols that may be used in the said kind of information with initial symbols, which are identical to the regularities used at encoding;
- extracting , from the encoded communication, of the data (R_i), defining the regularity which is used in the current transformation cycles and connects the values of the encoded communications with the concrete symbols of the transformed information of the current transformation cycle;
- selecting the regularity connecting the values of the encoded communications with the concrete symbols of the transformed information of the current transformation cycle;
- extracting from the accessory information (F) the accessory information for the said transformation cycle (F_i);
- transforming the transformed information (C_i) using the selected regularity and the accessory information for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;
- *characterised in that,* the accessory information for the said transformation cycle (F_i); is isolated from the array of the accessory information (F);
- recovering the information (C_i), which is transformed in the respective cycle, by using the selected regularity and the accessory information for the said transformation cycle (F_i);
- making decision on switching to the next cycle or termination of the transformation;

- using additionally in each transformation cycle a respective part of the accessory information, as a result of transforming with the use of the selected regularity there is formed the information recovered in the respective cycle.

8. The process of decoding the encoded information according to claims 7, *characterised in that*

- in each transformation cycle there is additionally used a respective part of the accessory information and as a result of transformation with use of the selected regularity there is formed a recovered in the corresponding cycle communication, the length of which is larger or equal to the length of the communication, resulting from transforming in the previous cycle.

9. The process of decoding the encoded information according to claims 7, *characterised in that*

in each transformation cycle there is additionally used a respective part of the accessory information, and as a result of transformation with use of the selected regularity there is formed a recovered in the respective cycle communication, the length of which is larger, equal or smaller than the length of the communication, resulting from transforming in the previous cycle.

10. The method according to claims 7, 8 or 9, *characterised in that*, the transformed in the respective cycle information (C_i) and/or the accessory information for the respective cycle (F_i) is preliminary unmixed in each cycle or in some cycles;

11. The device for realising the process for decoding information, comprises:

- an input unit,
- an output unit,
- data base on the regularities connecting the encoded information with the initial information,
- *characterised in that*, the device further comprises
- a transformation unit;
- a storage of the recovered communication;
- a storage of the accessory information;
- a making decision unit;
- a commutator,

the first input of the accessory information storage connected with first output of the input unit and the second input of the accessory information storage connected with first output a making decision unit; the first input of data base is connected to the second output of the of the input unit, and the second input – to the first output of the storage for accessory information; the first input of the storage of the recovered information is connected to the third output of the input unit, the second – to the output of the transformation unit, and the third – to the first output of the making decision unit, the first input of the transformation unit is connected to the second output of the storage of accesory information, and the second – to the output of database, the third to the first output of the storage of recovered information; the second - to the fourth output of the input unit, the first input of the commutator is connected to the second output of the making decision unit, and the second – to the second output of the making decision unit, the output unit is connected to the second commutator output .

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/06

A1

(11) International Publication Number: **WO 00/65767**

(43) International Publication Date: 2 November 2000 (02.11.00)

(21) International Application Number: PCT/BY99/00005

(22) International Filing Date: 27 April 1999 (27.04.99)

(71)(72) Applicant and Inventor: MISCHENKO, Valentin Alexandrovich [BY/BY]; 28–210, Nekrosova Str., Minsk, 220040 (BY).

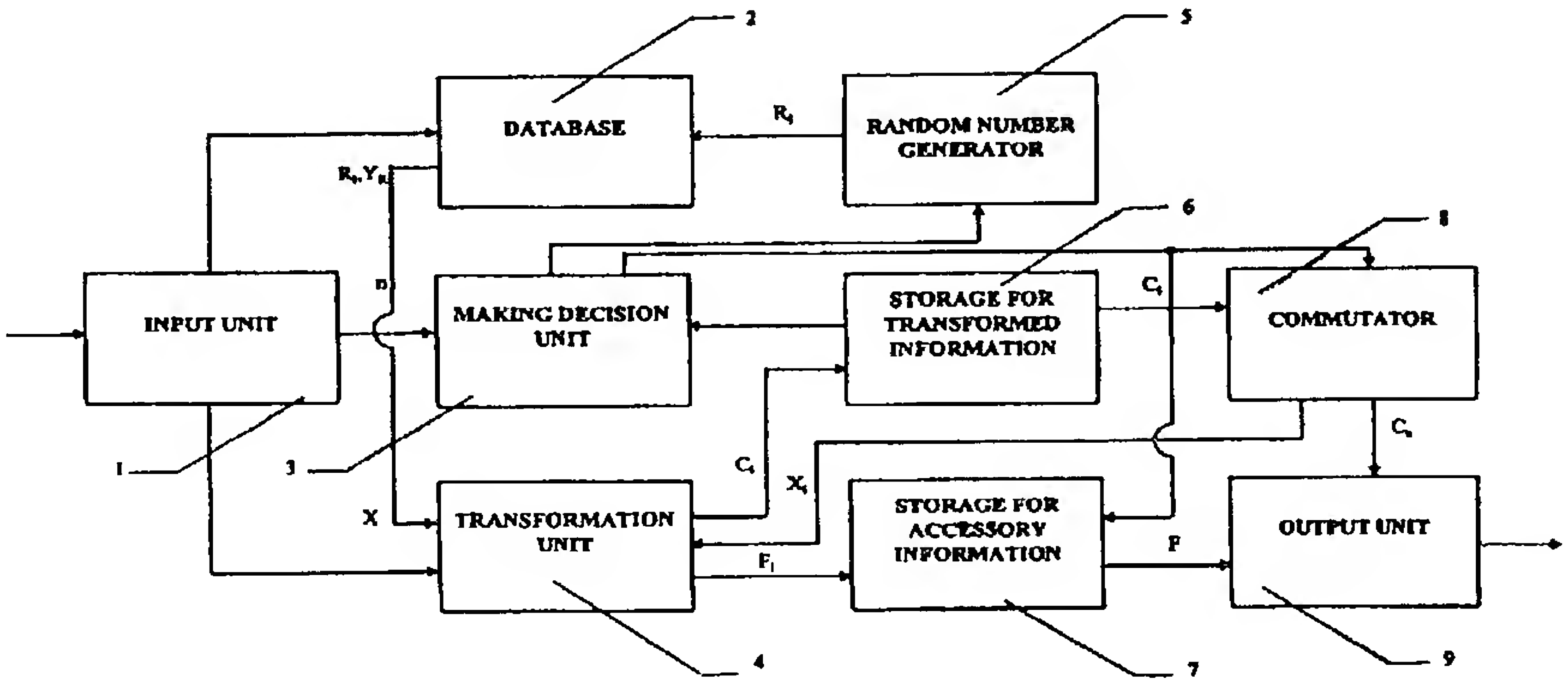
(72) Inventors; and
(75) Inventors/Applicants ***(for US only)*****:** ZAKHARAU, Uladzimir Uladzimirovich [BY/BY]; 1–2–22, 50 Let Pobedy Str., Minsk, 220056 (BY). VILANSKI, Yuri V. [BY/BY]; 10–44, Kuleshova Str., Minsk 220026 (BY). VERZHBALOVICH, Dzmitry I. [BY/BY]; Mvizru Pvo, Minsk 220057 (BY).

(74) Agent: VINOGRADOV, Sergei Gennadievich; P.O. Box 261, Minsk, 220006 (BY).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR ENCRYPTING INFORMATION AND DEVICE FOR REALIZATION OF THE METHOD



(57) Abstract

The invention relates to means for protecting information from an unauthorised access by electronic means. In order to transform the initial information the device has the transformation unit (4), the making decision unit (3), the storage of the recovered communication (6), the commutator (8), and for storing the accessory information the device has the storage of the accessory information (7). For encoding and transferring information the addressee is beforehand provided with a key to the received communications with information on regularities corresponding to the values of the communication transmitted to him, with specific values of the initial information for the whole set of symbols of the said kind of an information. In this case the addressee is beforehand provided with a set of transformation functions, Y_1, Y_2,..., Y_N = Y_i,(X), where X = {x_1, x_2,..., x_m} is a plurality of specific symbols of the transformed information. In the course of processing the encrypted information the input of the making decision unit (3) enters the information on the number (n) of transformation cycles of the initial communication. Before the beginning of the current transformation cycle, the making decision unit (3) transmits a control signal to the generator of random numbers (5), which generates a random number (Ri), transmits it to the data base (2) and through the latter to the transformation unit.

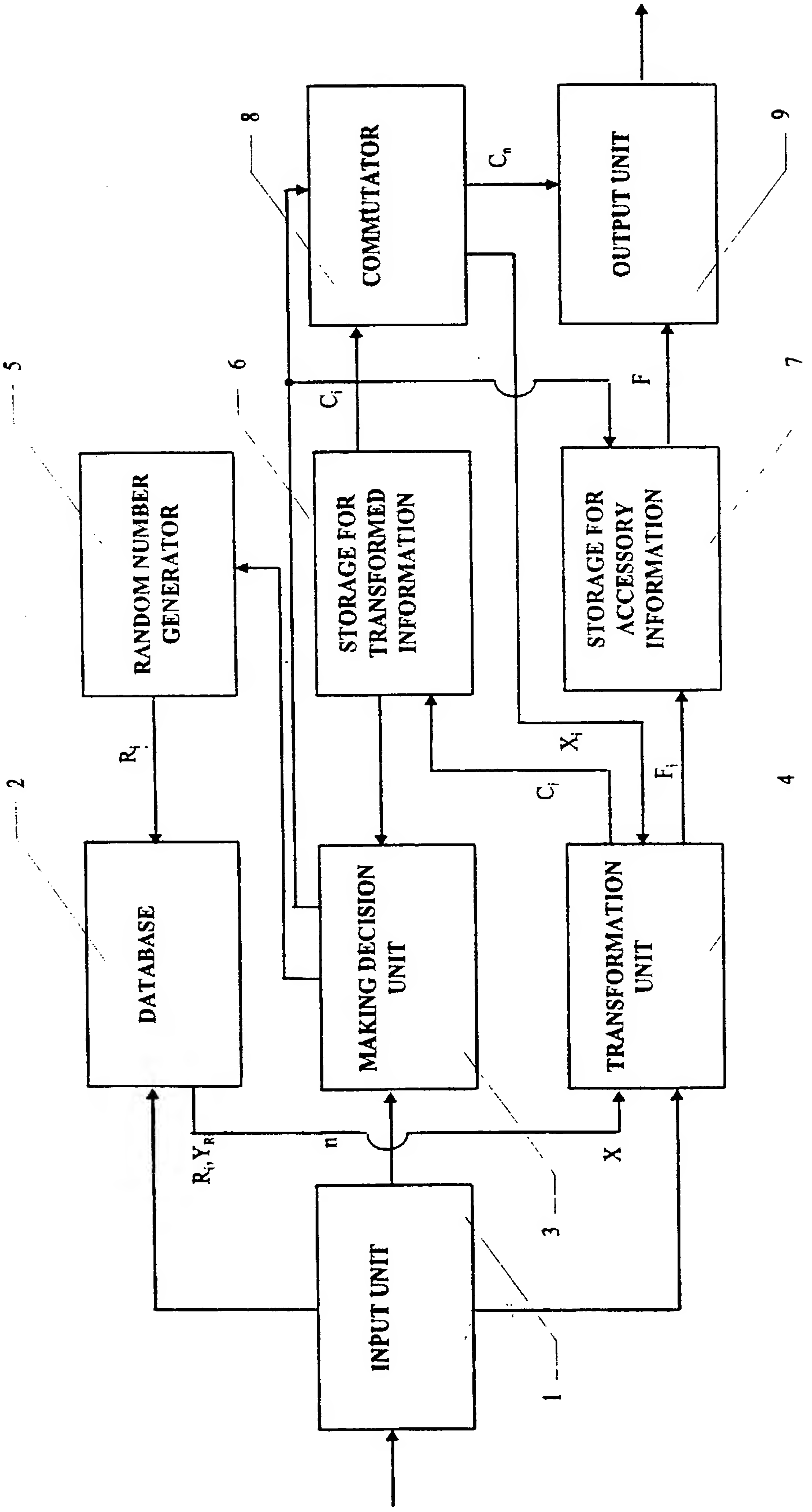

INPUT UNIT
DATABASE
MAKING DECISION UNIT
TRANSFORMATION UNIT
RANDOM NUMBER GENERATOR
STORAGE FOR TRANSFORMED INFORMATION
STORAGE FOR ACCESSORY INFORMATION
COMMUTATOR
OUTPUT UNIT
1
2
3
4
5
6
7
8
9
R_i, Y_R
n
X
R_i
C_i
X_i
F_i
C_i
F
C_n

FIG 1

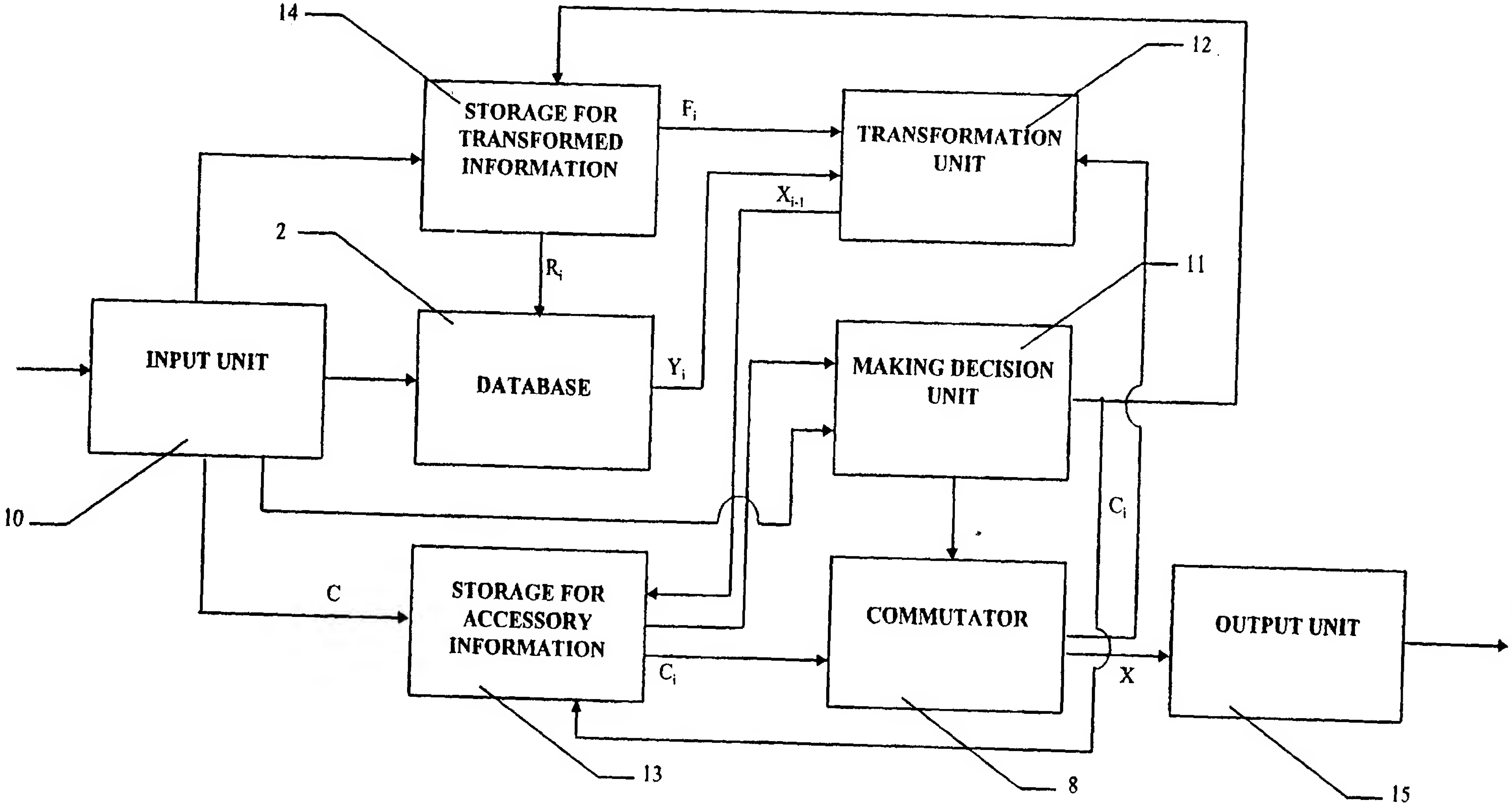

14
STORAGE FOR TRANSFORMED INFORMATION
F_i
12
TRANSFORMATION UNIT
X_{i-1}
2
R_i
11
INPUT UNIT
DATABASE
Y_i
MAKING DECISION UNIT
10
C_i
C
STORAGE FOR ACCESSORY INFORMATION
COMMUTATOR
OUTPUT UNIT
C_i
X
13
8
15

FIG. 2

PTO/SB/107 (5-95)
Approved for use through 9/30/98 OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respon" to a collection of information unless it displays a valid OMB control number.

Declaration and Power of Attorney for Patent Application

Заявление о подаче заявки на патент и доверенность поверенному

Заявлениe на русском языке

Russian Language Declaration

Я, нижеупомянутый изобретатель, настоящим подтверждаю, что:

Мое местожительство, почтовый адрес и гражданство действительно таковы, как указано ниже, непосредственно после моего имени.

Я убежден, что я являюсь первоначальным, первым и единственным изобретателем (если ниже указано только одно имя), или одним из первоначальных и первых со-авторов (если ниже указаны несколько имен) заявляемого изобретения, на которое запрашивается патент и которое называется:
СПОСОБ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ ИНФОРМАЦИИ
И УСТРОЙСТВО ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ

Описание изобретения приложено к сему (если в расположенной ниже клетке нет отметки):

□ было подано /дата/ 27.04.1999
как заявка США номер или международный PCT № PCT/BY99/00005
__________ с изменениями, внесенными /дата/
__________ (если требуется).

Настоящим я заявляю, что я изучил и понимаю содержание вышеназванного описания, включая формулу изобретения со всеми поправками, указанными выше.

Я признаю обязанность сообщить информацию, необходимую для патентования в соответствии с §1.56 раздела 37 Кодекса Федеральных Правил.

Настоящим я предъявляю иностранные преимущественные права приоритета в соответствии с §119 (a)-(d) или §365 (b) раздела 35 Кодекса *Соединенных Штатов* на любую(ые) иностранную(ые) заявку(и) на патент или авторское свидетельство, или с §365 (a) на любую международную заявку PCT, назначившую одну или больше стран кроме Соединенных Штатов, перечисленную(ые) ниже, а также указал ниже с расположением отметки в клетке все иностранные заявки на патент или авторское свидетельство или международную заявку PCT, поданные ранее, чем заявка, на которую предъявлено притязание на приоритет.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled
METHOD OF ENCODING AND DECODING INFORMATION
DEVICE FOR REALIZATION OF THE METHOD

the specification of which is attached hereto unless the following box is checked:

□ was filed on 27.04.1999
as United States Application Number or PCT International Application Number PCT/BY99/00005
__________ and was amended on
__________ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT international application which designated at least one country other than the *United States, listed below and have also identified below, by* checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Prior Foreign Application(s)
Прежняя(ие) иностранная(ые) заявка(и)

Притязание на приоритет не предъявляется

Priority Not Claimed

Номер (Number)	Страна (Country)	День/Месяц/Год подачи (Day/Month/Year Filed)	□
Номер (Number)	Страна (Country)	День/Месяц/Год подачи (Day/Month/Year Filed)	□
Номер (Number)	Страна (Country)	День/Месяц/Год подачи (Day/Month/Year Filed)	□

Настоящим я предъявляю иностранные преимущественные права приоритета в соответствии с § 119 (е) раздела 35 Кодекса Соединенных Штатов на любую(ые) предварительную(ые) заявку(и), перечисленную(ые) ниже.

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below.

(Заявка №) (Дата подачи заяки)

(Application No.) (Filing Date)

(Заявка №) (Дата подачи заяки)

(Application No.) (Filing Date)

Настоящим я заявляю претензию на выгоду, в соответствии с § 120 раздела 35 Кодекса Соединенных Штатов, от всех нижеперечисленных заявок(ки) США или с § 365 (с) от любой международной заявки РСТ, назначившей Соединенные Штаты, в той мере, в которой предмет изобретения в каждом пункте, на который заявлен приоритет, не был раскрыт в поданной ранее заявке США или международной заявке РСТ, как это предусмотрено в первом абзаце § 112 раздела 35 Кодекса Соединенных Штатов. Я признаю обязанность раскрыть информацию, которая является вещественной для патентоспособности, как это предусмотрено в § 1.56 раздела 37 Кодекса Федеральных Правил, которая стала доступна за период времени между подачей предшествующей заявки и датой подачи национальной или международной заяки РСТ.

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application

PTO/SB/107 (5-00)
Approved for use through 9/30/00 OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

(Заявка №) (Application No.)	(Дата подачи заявки) (Filing Date)	(Статус - запатентовано, рассматривается, заявитель отказался) (Status - patented, pending, abandoned)
(Заявка №) (Application No.)	(Дата подачи заявки) (Filing Date)	(Статус - запатентовано, рассматривается, заявитель отказался) (Status - patented, pending, abandoned)

Настоящим подтверждаю, что все заявления, сделанные здесь на основе моих знаний, являются правдой, и я также верю в достоверность всех заявлений, основанных на доступной мне информации и убеждениях; кроме того, эти заявления были сделаны со знанием того, что умышленно ложные заявления и подобные им действия караются штрафом, или тюремным заключением, или тем и другим, в соответствии со статьей 1001 раздела 18 Кодекса Соединенных Штатов, и что такие ложные сведения могут сделать недействительной как эту заявку, так и любой патент, по ней выданный.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

ДОВЕРЕННОСТЬ ПОВЕРЕННОМУ: В качестве названного здесь изобретателя, я уполномачиваю следующего(их) поверенного(ых) и/или агента(ов) подать эту заявку и осуществлять все операции с ней связанные в Ведомстве по Патентам и Торговым Знакам *(далее идет имя и регистрационный номер).*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: *(list name and registration number)*

David B. Newman, Jr.
Registration No. 30,966

D

Корреспонденцию посылать по адресу:

Send Correspondence to:

DAVID NEWMAN CHARTERED
P.O. BOX 2728
LA PLATA, MD 20646

По телефону обращаться к:
(имя и номер телефона)

Direct Telephone Calls to: (name and telephone number)

TEL: 301-934-6100

PTO/SB/107 (5-00)
Approved for use through 9/30/00 OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

МИЩЕНКО Валентин Александрович 1-00 MISCHENKO Valentin Alexandrovich

Полное имя единственного или первого автора изобретения — **Full name of sole or first inventor**

15 03.2002

Подпись автора изобретения — Дата — **Inventor's signature** — **Date**

Беларусь — Belarus

Местожительство — **Residence**

Беларусь — Belarus BYX

Гражданство — **Citizenship**

28-210, Некрасова, Минск 220040

Почтовый адрес — **Post Office Address**

ЗАХАРОВ Владимир Владимирович 2-00 ZAKHARAU Uladzimir Uladzimirovich

Полное имя второго автора изобретения (если имеется) — **Full name of second joint inventor, if any**

15 03 2002

Подпись автора изобретения — Дата — **Second Inventor's signature** — **Date**

Беларусь — Belarus

Местожительство — **Residence**

Беларусь — Belarus BYX

Гражданство — **Citizenship**

1-2--22, 50 лет Победы, Минск, 220056, — 1-2--22, 50 Let Pobedy Str , Minsk, 220056, Belarus

Почтовый адрес — **Post Office Address**

see next page

(Аналогичная информация о третьем и последующих авторах изобретения должна быть представлена, а также их подписи) — **(Supply information and signature for third and subsequent joint inventors.)**

ВИЛАНСКИЙ Юрий В. 3-00 VILANSKI Yuri V.

Полное имя единственного или первого автора изобретения — Full name of sole or first inventor

15 03 2002

Подпись автора изобретения — Дата — Inventor's signature — Date

Беларусь — Belarus

Местожительство — Residence

Беларусь — Belarus BYX

Гражданство — Citizenship

10-44, ул Кулешова, Минск, 222 — 10-44, Kuleshova Str., Minsk, Belarus 220026

Почтовый адрес — Post Office Address

ВЕРЖБАЛОВИЧ Дмитрий.И. 4-00 VERZHBALOVICH Dzmitry I.

Полное имя второго автора изобретения (если имеется) — Full name of second joint inventor, if any

15.03.2002

Подпись автора изобретения — Дата — Second inventor's signature — Date

Беларусь — Belarus

Местожительство — Residence

Беларусь — Belarus BYX

Гражданство — Citizenship

МВИЗРУ ПВО, Минск 220057 — MVIZRU PVO Minsk 220057

Почтовый адрес — Post Office Address

(Аналогичная информация о третьем и последующих авторах изобретения должна быть представлена, а также их подписи) — (Supply information and signature for third and subsequent joint inventors.)